Übungsblatt 11

Abgabe der schriftlichen Lösungen bis 14.07.2022, 24 Uhr

Aufgabe 55 Sei $(G, \cdot, 1)$ eine endliche Gruppe der Ordnung m. ***mündlich***

(a) Zeigen Sie, dass für jedes $a \in G$ die Menge $\langle a \rangle = \{a^i \mid i \geq 0\}$ eine Untergruppe von G mit genau $\mathrm{ord}(a)$ Elementen bildet. Folgern Sie $\mathrm{ord}(a) | m$ und $a^m = 1$.

(b) Zeigen Sie, dass für jedes $a \in G$ die Äquivalenz $a^i = a^j \Leftrightarrow i \equiv_{\mathrm{ord}(a)} j$ gilt.

(c) Zeigen Sie, dass $\mathrm{ord}(a^i) = \mathrm{ord}(a)/\,\mathrm{ggT}(\mathrm{ord}(a), i)$ für jedes $a \in G$ gilt.

(d) Geben Sie einen Isomorphismus zwischen den Gruppen $\langle a \rangle$ und $(\mathbb{Z}_{\mathrm{ord}(a)}, +)$ an.

(e) Bestimmen Sie für die Gleichung $a^x = b$ $(a, b \in G)$ alle Lösungen $x \in \mathbb{Z}_{\mathrm{ord}(a)}$.

Aufgabe 56 ***mündlich***

Seien a, b Elemente einer abelschen Gruppe G mit Ordnungen $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$.

(a) Zeigen Sie, dass ab die Ordnung $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$ hat, falls $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd sind. Gilt dies auch, wenn G nicht abelsch ist?

(b) Lässt sich die Aussage in Teilaufgabe (a) zu $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))$ oder zu $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))/\,\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b))$ verallgemeinern?

Aufgabe 57 ***mündlich***

(a) Zeigen Sie, dass ein Polynom $p(x) \in \mathbb{F}[x]$ vom Grad $n \geq 1$ über einem Körper $\mathbb{F}$ höchstens n Nullstellen besitzt.

(b) Folgern Sie, dass die Einheitengruppe $\mathbb{F}_q^*$ eines endlichen Körpers $\mathbb{F}_q$ zyklisch ist.

(c) Finden Sie Polynome $q_d(x) \in \mathbb{Z}_6[x]$ vom Grad $d = 0, 1, 2$ mit möglichst vielen Nullstellen.

(d) Zeigen Sie, dass ein Polynom $q_d(x) \in \mathbb{Z}_m[x]$ vom Grad $d \geq 1$ für quadratfreies $m \geq 2$ höchstens dm/p Nullstellen hat, wobei p der kleinste Primteiler von m ist. In welchen Fällen ist diese Schranke scharf?

Aufgabe 58 ***mündlich***

Berechnen Sie $\varphi(75\,600)$, $\varphi(14\,948)$, $\log_{7,3} 4$, $\log_{37,2} 3$, $\mathrm{ord}_7(2)$ und $\mathrm{ord}_{31}(2)$.

Aufgabe 59 Zeigen Sie: ***mündlich***

(a) Keine gerade Zahl n ist eine Carmichaelzahl.

(b) Für kein $k \geq 2$ und keine Primzahl $p > 2$ ist $n = p^k$ eine Carmichaelzahl.
(*Hinweis:* Zeigen Sie, dass $a = p^{k-1} + 1$ kein falscher Primzahlzeuge für n ist.)

(c) Jede Carmichaelzahl n ist quadratfrei.
(*Hinweis:* Zeigen Sie, dass $\mathrm{ord}_{p^2}(p+1) = p$ ist, und benutzen Sie im Fall $p^2 | n$ den chinesischen Restsatz zur Konstruktion einer Zahl $a \in \mathbb{Z}_n^*$ mit $a^{n-1} \not\equiv_n 1$.)

(d) Eine ungerade, zusammengesetzte und quadratfreie Zahl n ist genau dann eine Carmichaelzahl, wenn $p - 1$ für jeden Primteiler p von n die Zahl $n - 1$ teilt.

(e) Jede Carmichaelzahl n lässt sich in drei teilerfremde Faktoren $n_1, n_2, n_3 > 1$ zerlegen.

Aufgabe 60 ***mündlich***

Verifizieren Sie, dass 561, 1729, 2465, 172081, 294409 und 56052361 Carmichaelzahlen sind.

Aufgabe 61 ***10 Punkte***

Berechnen Sie die beiden Testmengen T_{221}^{FT} und T_{221}^{MRT} sowie die Menge U_{221}.